TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

SECTION 5
IPV6

5.1 INTRODUCTION

The overarching guidance is that all Internet protocol (IP) interfaces have to be dual stacked and meet the IPv6 requirements. All features and functionality available on IPv4 networks will need to be supported on IPv6 networks as well. While there are requirements to manage IPv6 networks, the Network Management may be done using IPv4, at this time.

The Department of Defense (DoD) Information Technology (IT) Standards Registry (DISR) baseline is updated to ensure that DoD capabilities for building and buying products are based on a current and effective set of IT National Security Space (NSS) standards. DoD IPv6 Standard Profiles for IPv6-Capable Products, version 6.0, is approved for distribution via the DISR for IPv6 for DoD IT equipment and for providing a seamless integration of Unified Capabilities (UC) applications (e.g., voice, video, chat/presence, data).

The DoD has also published core IPv6 standards implementation guidance for Joint Capabilities Integration and Development System (JCIDS) Net-Ready Key Performance Parameter (NR-KPP) compliance in the IPv6 Global Information Grid (GIG) Technical Profiles.

The Defense Information Systems Agency (DISA) IPv6 Transition Office (DITO), in conjunction with the National Security Agency (NSA), has published the security requirements for all IPv6-capable devices, systems, services, and networks. The Milestone Objective 3 (MO3) outlines filtering, configuration, and transition related guidance for network nodes in the enclave boundary, demilitarized zone (DMZ), and interior networks. MO3 allows for the coexistence of IPv4 and IPv6, natively and in tunnels, to traverse inside and across the DoD network boundary. The MO3 describes security safeguards. It is imperative that products fielded in operational environments are configurable and support the outlined security mechanisms. These requirements are not only for Information Assurance devices, but also include configuration items for other non-Information Assurance devices that perform, implement, or manage a security-related function (e.g., host, router). At a future date, IPv6 Information Assurance guidance from MO3 will be incorporated into revisions of the appropriate Security Technical Implementation Guideline (STIG).

5.2 DEFINITIONS

These definitions are derived from DoD Deputy Chief Information Officer (CIO) Memorandum, DoD IPv6 Definitions:

1. IPv6-Capable Products. Products (whether developed by a commercial vendor or the Government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments. The IPv6-capable products shall be able to

interoperate with other IPv6-capable products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6, and shall also do the following:

a. Conform to the requirements of the IPv6 profile in the Unified Capabilities Requirements (UCR).

b. Possess a migration path and/or letter of commitment to upgrade from the developer (signed by the company vice president or equivalent) as the IPv6 standard evolves.

c. Ensure that product developer IPv6 technical support is available.

d. Conform to NSA and/or Unified Cross Domain Management Office requirements for Information Assurance products.

2. System Under Test (SUT). The inclusive components required to test a UC product for Approved Products List (APL) certification. Examples of a System Under Test (SUT) include Voice over Internet Protocol (VoIP) system components (e.g., Session Controller [SC] and Gateway), Local Area Network (LAN) components (e.g., routers and Ethernet switches), and end instruments (EIs).

3. IPv6-Capable Networks. Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only IPv4, only IPv6, or both IPv4 and IPv6. An IPv6-capable network shall be ready to have IPv6 enabled for operational use when mission need or business case dictates. Specifically, an IPv6-capable network must do the following:

   a. Use IPv6-capable products.

   b. Accommodate IPv6 in network infrastructures, services, and management tools and applications.

   c. Conform to DoD- and NSA-developed IPv6 network security implementation guidance.

   d. Manage, administer, and resolve IPv6 addresses in compliance with the DoD IPv6 Address Plan when enabled.

4. IPv6-Enabled Network. An IP network that is supporting operational IPv6 traffic through the network, end-to-end.

Figure 5.2-1, IPv6 Design for SBU and Classified VVoIP, depicts the IPv6 network design for SBU and classified Voice and Video over IP (VVoIP), and includes the Defense Information Systems Network (DISN) Service Delivery Nodes (SDNs). All UC-approved products will be IPv6 capable, and the VVoIP network will be an IPv6-enabled network during Spiral 2 of its capabilities deployments.

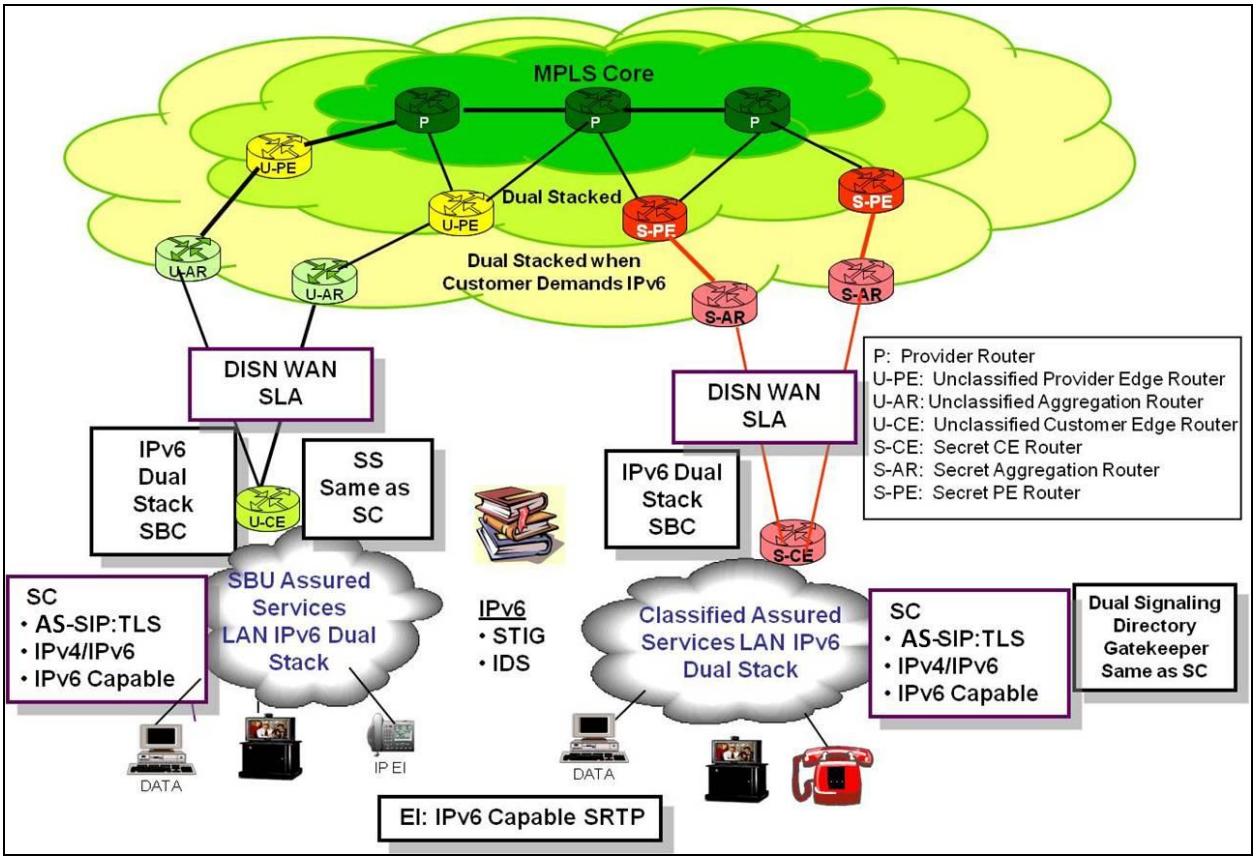

Figure 5.2-1. IPv6 Design for SBU and Classified VVoIP

5.3 DoD IPV6 PROFILE

DoD IPv6 Standard Profiles for IPv6 Capable Products, version 6.0, defines various LAN switches as follows:

1. Layer 2 Switch. A switch that forwards based on Layer 2 only (Media Access Control [MAC] address). Note that an unmanaged Layer 2 switch can be described as a "pure" Layer 2 switch; it operates at Layer 2 only and is transparent at the IP layer. As such, it has no IPv6-specific requirements and plays no active role as an IPv6-capable product. A Layer 2 switch may have some limited Layer 3 control plane functions but is primarily a data plane device. A managed Layer 2 switch product includes Simple Network Management Protocol (SNMP) management or other user access via an IPv6 interface, and it should be evaluated as a Simple Server.
2. Layer 3 Switch. A switch that incorporates Layer 3 information (IP addresses) into forwarding decisions. Forwarding may be manually configured, policy based, or based on routing protocols (Border Gateway Protocol [BGP], Routing Information Protocol [RIP], Open Shortest Path First version 3 [OSPFv3], or Intermediate System to Intermediate System [IS-IS]). Most Layer 3 switches require a router gateway to connect the LAN/Intranet to the

Internet. The most capable Layer 3 switches include a Wide Area Network (WAN) interface and an exterior routing protocol such as BGP.

3. Assured Services Switch. A switch that includes support for Quality of Service (QoS) features including the Differentiated Services Code Point (DSCP) queuing (Request for Comments [RFC] 2474). The DSCP queuing is an essential capability in the Unified Communications architecture to provide for Assured Services. Rather than being a separate product class, the requirements for Assured Services are specified as Conditional Requirements for compatibility with the UCR.

For the UCR, this third category of switch is called a LAN Access Switch, which is required to support RFC 2460/5095 and RFC 2464, and must be able to queue packets based on DSCPs in accordance with RFC 2474. If the application of the LAN Access Switch is a Layer 2 Switch, then it can be actively managed and supports queuing via DSCP, but not actually required to route. The complete set of RFCs for LAN switches is listed in UCR 2013, Section 5, Table 5.2-6, LAN Switch (LS). Part 1 is LAN Access Switch, Part 2 is LAN Distributed Switch, and Part 3 is LAN Core Switch.

5.3.1 Product Requirements

As mentioned in UCR 2013, Section 2, Session Control Products, the Unified Capabilities Requirements are the minimum set of requirements necessary for the system to be IPv6 capable for VVoIP.

As the evolution of IPv6 continues and industry-wide adoption of the same increases, the DoD community may consider other features and capabilities for IPv6 such as the following:

- Simple Mail Transfer Protocol (SMTP) IPv6 network management.
- Multicasting features to support IPv6 addressing and the service function of multicasting.
- Possible use of anycast addresses.
- Tactical, deployable, mobile IPv6.
- Ad hoc networks (such as Mobile Ad Hoc Network [MANET]).

Requirement for the use of such features will be defined in subsequent updates to the UCR 2013 based on the needs identified by the DoD community.